BlueCasa COMMUNICATIONS

Your New Home Phone Company

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Blue Casa Communications, Inc.

FRN: 0009051731

I, Brian Plackis, certify that I am an officer of Blue Casa Communications, Inc. (the "Company"), am authorized to make this certification on its behalf, and that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with Section 222 of the Communications Act of 1934 and the Federal Communications Commission rules implementing Section 222.

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 24.2001 *et seq.* of the Commission's rules.

The Company has not taken any actions (proceedings instituted or petitions filed by the company at either state commission, the court system, or at the Commission) against data brokers in the past year.

The Company has industry knowledge and an understanding of the processes that pretexters are using in attempts to access CPNI. The steps the Company is taking to protect CPNI are described in the attached statement.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

By: 

Brian Plackis

Title: COO

Dated: February 27, 2009

STATEMENT OF COMPLIANCE PROCEDURES

Blue Casa Communications, Inc. (the "Company") has established operating procedures to protect the privacy of Customer Proprietary Network Information ("CPNI") as follows:

(1) The Company does not allow the use of CPNI for sales or marketing of any category of service to which a customer does not already subscribe, except for the provision of CPE, voice mail, inside wire service, or custom-calling (adjunct-to-basic) services. The Company has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI for sales or marketing purposes. Any outbound marketing request for customer approval for the use of CPNI requires supervisory authorization under an established supervisory review process designed to ensure compliance with the Commission's CPNI rules in outbound marketing situations. The Company maintains, for a minimum of one year, a record of its and its affiliates' sales and marketing campaigns that use customers' CPNI. The Company also maintains, for a minimum of one year, a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.

(2) The Company has adopted authentication procedures to protect against unauthorized access to CPNI during customer-initiated telephone contact, online account access, and visits to the Company's business locations at which access to CPNI may be obtained. These procedures require the customer to provide, in the case of visits to the Company's locations, a proper photo i.d., and in other cases, a password that is provided to the customer only after the customer is first authenticated using non-readily-available biographical or account information. Further, whenever a password, response to back-up means of authentication, online account, or address of record is created or changed, the customer is notified of the change in accordance with the FCC's rules safeguarding CPNI. In cases where a business customer has a dedicated Company account representative, other authentication methods may be used as expressly set forth in the contract between the Company and the customer.

(3) Except as set forth above, the Company discloses CPNI to third parties only pursuant to lawful process. In the event of any uncertainty, the Company's policy is to consult with counsel before responding to any request for CPNI from a third party.

(4) In the event of any breach in the security of customers' CPNI, the Company will notify law enforcement pursuant to the FCC's rules before notifying customers or publicly disclosing the breach. In addition, the Company will maintain records of all such breaches and notifications as required by the FCC's rules.

2) The Company has trained all personnel who have access to CPNI, or control over access to CPNI, regarding the uses for which CPNI may be made, the restrictions in the use of CPNI, and the authentication requirements for disclosure of CPNI to customers, and all personnel have been trained in the notification procedures to be followed in the event of a breach. The Company has a no tolerance policy for violations and will discipline any individual who has been found in violation of CPNI requirements. Intentional or grossly-negligent violations will result in termination. In other cases, discipline, up to and including termination, will apply, as appropriate.

BlueCasa COMMUNICATIONS

Your New Home Phone Company

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Blue Casa Communications, Inc.

FRN: 0009051731

I, Brian Plackis, certify that I am an officer of Blue Casa Communications, Inc. (the "Company"), am authorized to make this certification on its behalf, and that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with Section 222 of the Communications Act of 1934 and the Federal Communications Commission rules implementing Section 222.

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 24.2001 *et seq.* of the Commission's rules.

The Company has not taken any actions (proceedings instituted or petitions filed by the company at either state commission, the court system, or at the Commission) against data brokers in the past year.

The Company has industry knowledge and an understanding of the processes that pretexters are using in attempts to access CPNI. The steps the Company is taking to protect CPNI are described in the attached statement.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

By: 

Brian Plackis

Title: COO

Dated: February 27, 2009

STATEMENT OF COMPLIANCE PROCEDURES

Blue Casa Communications, Inc. (the "Company") has established operating procedures to protect the privacy of Customer Proprietary Network Information ("CPNI") as follows:

(1) The Company does not allow the use of CPNI for sales or marketing of any category of service to which a customer does not already subscribe, except for the provision of CPE, voice mail, inside wire service, or custom-calling (adjunct-to-basic) services. The Company has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI for sales or marketing purposes. Any outbound marketing request for customer approval for the use of CPNI requires supervisory authorization under an established supervisory review process designed to ensure compliance with the Commission's CPNI rules in outbound marketing situations. The Company maintains, for a minimum of one year, a record of its and its affiliates' sales and marketing campaigns that use customers' CPNI. The Company also maintains, for a minimum of one year, a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.

(2) The Company has adopted authentication procedures to protect against unauthorized access to CPNI during customer-initiated telephone contact, online account access, and visits to the Company's business locations at which access to CPNI may be obtained. These procedures require the customer to provide, in the case of visits to the Company's locations, a proper photo i.d., and in other cases, a password that is provided to the customer only after the customer is first authenticated using non-readily-available biographical or account information. Further, whenever a password, response to back-up means of authentication, online account, or address of record is created or changed, the customer is notified of the change in accordance with the FCC's rules safeguarding CPNI. In cases where a business customer has a dedicated Company account representative, other authentication methods may be used as expressly set forth in the contract between the Company and the customer.

(3) Except as set forth above, the Company discloses CPNI to third parties only pursuant to lawful process. In the event of any uncertainty, the Company's policy is to consult with counsel before responding to any request for CPNI from a third party.

(4) In the event of any breach in the security of customers' CPNI, the Company will notify law enforcement pursuant to the FCC's rules before notifying customers or publicly disclosing the breach. In addition, the Company will maintain records of all such breaches and notifications as required by the FCC's rules.

2) The Company has trained all personnel who have access to CPNI, or control over access to CPNI, regarding the uses for which CPNI may be made, the restrictions in the use of CPNI, and the authentication requirements for disclosure of CPNI to customers, and all personnel have been trained in the notification procedures to be followed in the event of a breach. The Company has a no tolerance policy for violations and will discipline any individual who has been found in violation of CPNI requirements. Intentional or grossly-negligent violations will result in termination. In other cases, discipline, up to and including termination, will apply, as appropriate.